Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 695–705
DOI : 10.47974/JDMSC-1742

Secret image scrambling and DWT-based image steganography using smoothing operation and convolution neural networks

Vijay Kumar Sharma *
Pramendra Kumar †
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur
Rajasthan
India

Sunita Singhal §
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur
Rajasthan
India

Bhanu Pratap Soni ‡
SEEE
College of Engineering, Science & Technology
Fiji National University
Nasinu
Fiji

Praveen Kumar Shukla @
Department of Computer and Communications Engineering
Manipal University Jaipur
Jaipur
Rajasthan
India

* *E-mail:* Vijaymayankmudgal2008@gmail.com (Corresponding Author)
† *E-mail:* pramendrakumarpti@gmail.com
§ *E-mail:* sunita.singhal@jaipur.manipal.edu
‡ *E-mail:* bhanu.soni@fnu.ac.fj
@ *E-mail:* praveen.shukla@jaipur.manipal.edu

Abstract

Steganography is known as a secret data sharing technique. It is a method of data protection which allows the user to send the information in enveloped form. That means the hidden data cannot be seen by the observer because one can only see the enveloped media. This paper presents a steganography technique using Pixel swapping-Quantum Hilbert image scrambling and discrete wavelet transformation, followed by stego image smoothing operation. Initial steps of proposed image steganography include best suitable cover image selection for secret image. This process compares the secret image with the different cover image presents in senders cover image database. Before embedding (encoding), the secret image is scrambled, and then performs the DWT transformation on this scrambled image and cover image. Next steps embed both resultant images and generate a new image named as stego image.

The picture quality of stego image is increased using pixel swapping based operation. The Decoding process of proposed steganography scheme is just reverse of the former encoding process followed by application of Convolutional neural networks (CNN) to improve the extracted secret image quality. The results show the strength of the proposed technique.

Subject Classification: *94A08 Image processing (compression, reconstruction, etc.) in information and communication theory.*

Keywords: *Quantum image scrambling, DWT, Steganography, Pixel swapping, security, CNN.*

1. Introduction

There are so many techniques to protect the data that come under information system security. Information system security can be broadly divided into 3- classes, cryptography [1], watermarking [2], steganography [3]. Information system security classified can be seen by following Figure 1.

Cryptography: In cryptography, we apply a technique to scramble the text or replace the alphabet with other characters. Thus, no one can

Figure 1

Information system security view

identify the meaning of a secret message, but one can identify that the message is going as an encrypted form [1], [2].

Watermarking: watermarking is a class of information hiding in which we can hide the watermark to shield the data from forgery [2].

Steganography: when we are talking about the secret sharing the first nameis a strike in mind, that is, steganography. It is used for secret communication of data or valuable information. It is applicable in all media like image, audio, or video files. One can embed the files in by selecting any digital media as cover and secret media.

Steganography attack: steganalysis is an attack on the steganography technique which the aim is to identify the inside Information [4].

2. Literature Review

Numerous secure data transfer schemes have been proposed day by day. Steganography paly big role to secure data transfer. A steganography scheme is called good steganography scheme if and only if there is no change is obtained by eyes in cover media after performing the embedding of secret information [5]. On the embedding approach steganography is grouped into two broad categories: Special domain and transfer domain [6]. Transfer domain is more robust as compared to special domain. In transfer domain, direct secret data imbedding is avoided while in special domain information is embedded into the cover image pixels. This difference makes the transfer domain more robust than the special domain. Lots of transfer domain schemes are possible, DWT [3], contourlet transform [7].

3. Proposed Scheme

The proposed data hiding approach has three most important process

(a) Best suitable cover image selection and secret image denoising.

(b) Steganography embedding and

(c) Secret data Extraction process.

Process (a), best suitable cover image selection is based on side-by-side comparison of secret image with the different cover images which are present in the sender database. This comparison is done by comparing these images on different parameters Peak signal-to- noise ratio (PSNR)[3], Normalized cross correlation NCC[3]. This makes the technique stronger. Secret image denoising process remove the noise using image filtering process, if any kinds of noise is present in the secret image.

The complete embedding process (process (a) and process (b)) is displayedin Figure 2

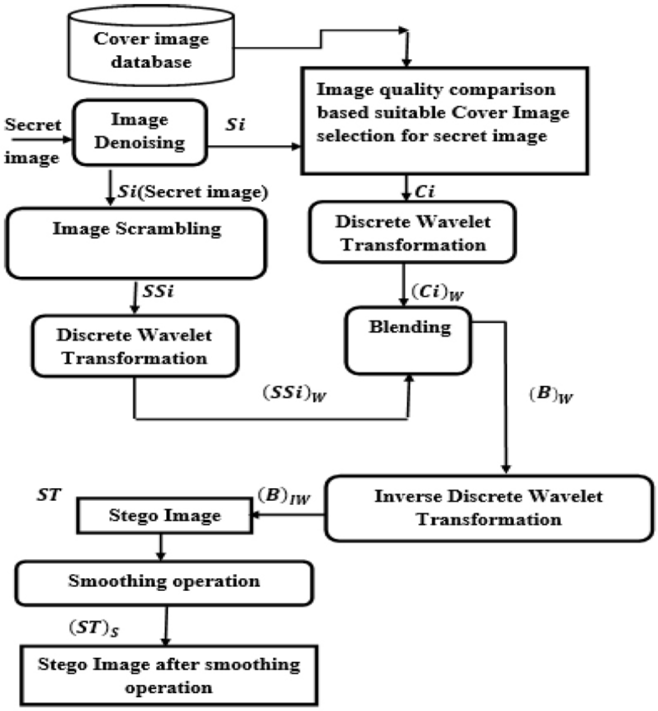


Figure 2

Embedding process of the proposed scheme

The earlier steps of embedding shown in Figure 3, secret image is scrambled using pixel swapping followed by Quantum image scrambling. That mean initially we perform pixel swapping operation on secret image which destroyed the secret image quality. Then we apply Quantum image scrambling [8][9], to generate final scrambled image. Thus, in proposed technique secret image is scrambled using following two steps

(i) pixel swapping, (ii) Quantum image scrambling

The septs involved in pixel swapping are as follows

Pixel swapping:

Pixel swapping interchange the nearby pixel, which are presented in following example for secret image SI. After applying pixel swapping operation scrambled image is generated which is shown by SI.

$$SI(:, [92\ 235]) = SI(:, [235\ 92])$$

Above look exchange the pixel position (235 92) and (92 235).

Algorithmic steps for pixel swapping are shown as follows for SI mage for a secret image matrix dimension R x C.

```
Pixel swapping algorithmic steps
C = number of columns
for (I = 1; i <= C/2; i++)
{
SI(:,[i C]) = SI(:,[C i]);
C= C-1;
}
```

Quantum image scrambling:

Quantum image scrambling. Quantum scrambling is also known as Hilbert image scrambling method [8][9], in this input image is passed through different quantum circuits to generate the scrambled image [8] [9]. Let's take an example, *Xn* is an image of size 128 X 128 (here *Xn* = *SI*). It can be represented as 27 X 27, and has multiple pixel information ranging from 1 to 2^{2n} pixels (n is 7). The different values of *Xn* can show in the below matrix.

$$Xn = \begin{pmatrix} 1 & 2 & 3 & \cdots & 4 \\ 2^n+1 & 2^n+2 & 2^n+3 & \cdots & 2^{n+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 2^{2n-1}+1 & 2^{2n-1}+2 & 2^{2n-1}+3 & \cdots & 2^{2n} \end{pmatrix}$$

The scrambling process, the scrambled version is the permutation of the original matrix *Xn*, lets assume that Hilbert matrix is represented by SSi. Table1 shows the correlation between original image baby.jpg and scrambled image pixel positions.

Table 1

Pixel position of the original image matrix and its corresponding Hilbert matrix

Original image matrix	Hilbert matrix
$X_0 = (10)$	$SSi_0 = (10)$
$X_1 = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$	$SSi_1 = \begin{pmatrix} 2 & 3 \\ 5 & 4 \end{pmatrix}$
$X_2 = \begin{pmatrix} 10 & 20 & 30 & 40 \\ 50 & 60 & 70 & 80 \\ 90 & 100 & 110 & 120 \\ 130 & 140 & 150 & 160 \end{pmatrix}$	$SSi_2 = \begin{pmatrix} 10 & 20 & 150 & 160 \\ 40 & 30 & 140 & 130 \\ 50 & 80 & 90 & 120 \\ 60 & 70 & 100 & 110 \end{pmatrix}$

Scrambling operation before the embedding improve the security of the proposed scheme. After the scrambling operation, DWT is applied to both the scrambled image and cover image, and we get the different frequency components of both images. In next, these frequency components are mixed using blending operation and we get a new image matrix.

The formulation of blending is shown below:

$$(B)_W = (Ci)_w + \alpha(SSi)_W \tag{1}$$

Here, $(B)_W$ represents the image information after the blending procedure, and $(Ci)_w$ and $(SSi)_W$ imply the cover image and the scrambled secret image, respectively. In the expression, α (alpha) implies a mixing factor.

After performing inverse wavelet transformation (IDWT) operation on this new image matrix, stego image (ST) is generated.

Finally, the stego image picture quality is improved using the smoothing operation. This is the pixel-based operation, in which the pixel intensity is updated using some set of rules, which is shown in table 2.

Table 2

Smoothing operation to improve the stego picture quality

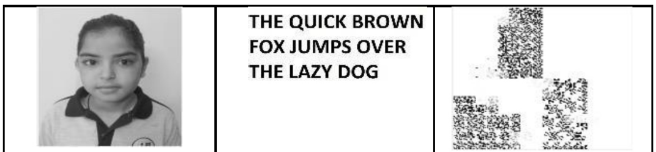
First Pixel value	Second pixel value
52 (No Change)	91 (No change)
53 (Swap first LSB)	90 (Swap first LSB)

This smoothing operation is applied on every two adjacent pixels and a new pixel pair is generated. Out of these, best suitable pixel pair is selected which has the minimum difference. And then shift the pixel position by onepixel right and repetitively apply this process to complete image. Finally, the best quality stego image (stego after smoothing operation) is generated. This image is sent to the receiver.

Receiver's end reverse process is applied to get the secret image.

4. Results an Analysis

The proposed DWT and smoothing operation-based steganography technique is executed in Matlab2019a. Performance of the proposed technique are measured on different testing parameters. Figure 3 represents an image 'pari.jpg' and 'pangram.jpg, which are carried as cover image and secret image respectively at alpha equal to 0.009.



(a)	(b)	(c)

Figure 3

(a) Cover image, (b) Secret image, (c) scrambled image

The stego image later smoothing operation, and extricated secret image aredisplayed in Figure 4.

(a)	(b)	(c)

Figure 4

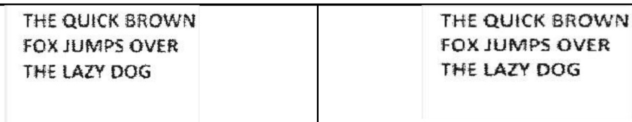
Image generation after embedding and extraction process. (a). Stego image (b). Stego image after smoothing operation (c). Extracted Secret image.

From Figure 4(c), it can be illustrated that a good quality extracted secret image is generated from the proposed scheme. The picture feature of obtained secret image(extracted secret image) can be enhanced using application of Convolutional neural networks (CNN) model [10].

Improvement in Extracted Secret image Quality using CNN

In next step the secret image picture quality is improved using application of the CNN model [10]. Convolutional neural networks (CNN) [10] are an effective tool to use to classify the image. Its hierarchical structure and excellent feature extraction features makes the model dynamic for improving the image quality. In this the layers organized in three dimensions (i.e. height, width and depth). CNN executes numerous convolutions and pooling processes to evaluate and monitor possible features using kernel function to extract the potential features of image [11] using the application of CNN.

Figure 5 shows the original obtained Secret image and obtained Secret image generated after applying CNN.



(a). Obtained Secret image	(b). Obtained Secret image after CNN

Figure 5

Extracted secret image before CNN and after applying CNN

Performance Analysis

The performance of the proposed technique is tested by executing it. To measure the performance, results on the following paraments have been calculated.

(i) PSNR [3],[12],[13], (ii) NCC [3],[12]

In table 3, the proposed technique columns before smoothing and after smoothing results are shown for PSNR and NCC.

Table 3

Comparative results of PSNR and NCC for same secret image Pangram.jpg

Cover image	PSNR		NCC	
	Before Smoothing operation	After smoothing operation	Before Smoothing operation	After Smoothing
Flower.jpg	41.2502	43.9061	0.9863	0.9909
Peppers.tiff	40.8495	43.2671	0.9864	0.9904
Lenna.tiff	41.0704	43.5137	0.9859	0.9901
Pirate.tiff	40.6991	43.4217	0.9845	0.9897

From above table 3, it is cleared that our technique gives better results. The observed range of PSNR before smoothing is 41Db to 43 Db and after smoothing it is near to 43 db, and also, technique gives the better NCC results.

In next, comparison of the proposed scheme is represented in table 4, with other existing technique [14].

Other well-known image excellence measure is Structural Similarity Measure (SSIM). It defines the structure similarity of 2 images [14].

Table 4

Comparative results of PSNR and SSIM with the proposed scheme and existing scheme by taking image Baboon as secret image size (256*256).

Cover image	Quality metrics	Existing Technique [14]	Proposed Technique	
			Before Smoothing operation	After smoothing operation
GoldHill (256*256)	PSNR	44.98	46.9594	48.9779
Lenna (256*256)		42.87	46.3238	47.7491
Barbara (256*256)		44.84	46.0631	48.1191
GoldHill (256*256)	SSIM	0.9896	0.9998	0.9996
Lenna (256*256)		0.9625	0.9625	0.9622
Barbara (256*256)		0.9921	0.9623	0.9618

From above table 4, it is cleared that our technique gives the better results than other existing techniques. It is also clearly seen from the table that stego image picture quality can be increased using the smoothing operation around 2 Bb.

6. Conclusion

This paper gives the details study about the different data protection schemes. Steganography was used in earlier days but in modern digital word watermarking and cryptography invented and play big role of data protection. The use of secret image scrambling before the embedding increases the security data protection. Stego image picture quality can be increased around 2%. using the smoothing operation in proposed work. Our technique provides good results as matched to the previous existing techniques. In feature work we will focus on a more robust data hiding methods.

References

[1] Manjit Kaur, Dilbag Singh, Kehui Sun, Umashankar Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map", *Future Generation Computer Systems*, Volume 107, Pages 333-350 (2020).

[2] Sharma, J.B., Sharma, K.K. & Sahula, V. Digital image dual watermarking using self-fractional fourier functions, bivariate empirical mode decomposition and error correcting code. *J Opt* 42, 214–227 (2013).

[3] Shikha Chaudhary, Saroj Hiranwal Chandra Prakash Gupta, "Spectral Graph Wavelet Based Image Steganography Using SVD and Arnold Transform ", *Traitement du Signal* Vol. 38, No. 4, (August, 2021), pp. 1113-1121.

[4] Subhedar, M.S., Mankar, V.H. Secure image steganography using framelet transform and bidiagonal SVD. *Multimedia Tools and Applications*, 79: 1865-1886 (2020).

[5] Behbod Keshavarzi, Behnam Zarpak, Seyed Hamid Haj Seyed Javadi & Gholam Reza Jandaghi. Adaptive steganography based on integer wavelet transform using block standard deviation, *Journal of Information and Optimization Sciences*, 40:7, 1457-1473 (2019), DOI: 10.1080/02522667.2018.1522797.

[6] Ye J, Ni J, Yi Y. Deep learning hierarchical representations for image steganalysis. *IEEE Trans Inf Forensics Secur* 12(11) : 2545–2557 (2017).

[7] Da Cunha AL, Zhou J, Do MN. The nonsubsampled contourlet transform: theory, design, and applications. *IEEE Trans Image Process* 15(10):3089–3101 (2006).

[8] B. Debnath, J. C. Das and D. De, "Reversible logic-based image steganography using quantum dot cellular automata for secure nano communication," in *IET Circuits, Devices & Systems*, Vol. 11, No. 1, pp. 58-67 (1 2017).

[9] Nan Jiang · LuoWang ·Wen-Ya Wu, "Quantum Hilbert Image Scrambling", *Int J Theor Phys*, Vol. 53, issue 7, pp 2463–2484 (2014).

[10] Schaeffer Koetter, J., Yan, J., Ortega, C. *et al.* Convolutional neural networks for improving image quality with noisy PET data. *EJNMMI Res* 10, 105 (2020).

[11] Gu J, Wang Z, Kuen J, Ma L, Shahroudy A, Shuai B, Liu T et al. Recent advances in convolutional neural networks. *Pattern Recogn* 77:354–377 (2018).

[12] Rathore M, Shekhawat NS, "Improved performance of image steganography technique using quantum scrambling and pixel's intensity adjustment". *Int J Future Evol Comput Sci Commun Eng* 5(8), (2019).

[13] Setiadi DIM. PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimed Tools Appl* 80 : 8423–8444 (2021).

[14] Kumar, V., Kumar, D. A modified DWT-based image steganography technique. *Multimedia Tools Appl*., 77: 13279-13308 (2018).